KETAHANAN *WATERMARKING* TERHADAP SERANGAN KOMPRESI JPEG

Aris Sugiharto dan Helmie Arif Wibawa
Jurusan Matematika FMIPA UNDIP
Jl. Prof. H. Soedarto, S.H, Semarang 50275

Abstract. Watermarking is one of the methods that proposed to protected digital data from illegally copy. A lot of technic to destroy watermarking that inserted to digital data, one of them are JPEG compression. In this research will be focus as far JPEG compression can influence watermarking integrated especially at similarity test before and after digital data have JPEG compression attact.

Keywords: watermarking, watermark, JPEG compression, similarity test.

1. PENDAHULUAN

Data digital pada era sekarang ini mengalami perkembangan yang sangat pesat. Banyak data digital dipertukarkan untuk berbagai kepentingan. Mulai dari kepentingan yang positif hingga kepentingan yang negatif. Salah satunya adalah adanya penggandaan secara illegal seperti pembajakan CD, konflik kepemilikan citra digital dan sebagainya. Hal inilah yang mengakibatkan data digital menjadi salah satu pusat perhatian karena kemudahan data ini untuk digandakan tanpa takut atau khawatir akan adanya penurunan kualitas [2]. Sehingga banyak upaya atau metode yang dikembangkan guna melindungi data digital dari upaya penggandaan di atas.

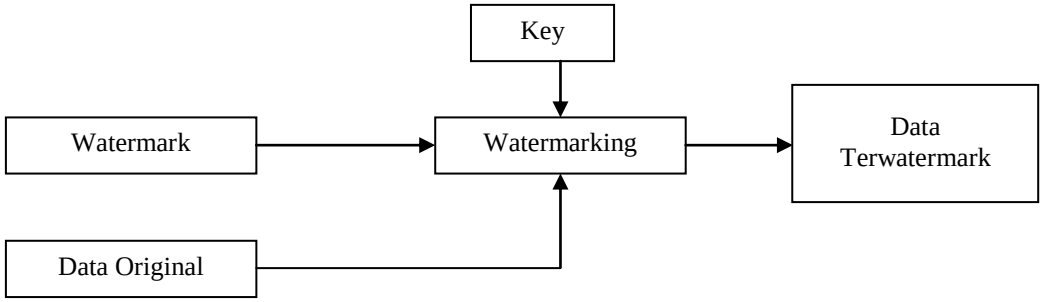
Watermarking hadir sebagai salah satu alternatif untuk melindungi data digital dari usaha orang-orang yang tidak bertanggung jawab yang dengan seenaknya tanpa memperhatikan hak atas kekayaan intelektual (HAKI) dengan melakukan upaya manipulasi dan penggandaan tanpa ijin. Akan tetapi *watermarking* dalam kenyataannya juga sangat sering mengalami berbagai serangan. Serangan ini dapat berupa serangan alamiah yaitu pemrosesan citra pada umumnya seperti proses rotasi, translasi, maupun cropping serta serangan yang tidak alamiah yang benar-benar bertujuan untuk menghilangkan *watermark*. Salah satu serangan ini adalah kompresi JPEG. Pada penelitian ini diinginkan untuk mengetahui seberapa jauh efek serangan ini terhadap keutuhan *watermark*.

2. TINJAUAN PUSTAKA

2.1. *Watermarking*

Watermarking merupakan sebuah metode yang relatif baru yang dimanfaatkan untuk melindungi data digital dari upaya penggandaan atau manipulasi secara illegal. *Watermarking* atau tanda air berbeda dengan tanda air pada uang kertas. Tanda air pada uang kertas masih dapat dilihat dengan mata telanjang (pada posisi tertentu), tetapi *watermarking* pada data digital tidak akan dirasakan kehadirannya oleh manusia tanpa menggunakan alat bantu mesin pengolah digital seperti komputer dan sejenisnya. Jadi *watermarking* dapat diartikan sebagai suatu teknik menyembunyikan data atau informasi "rahasia" ke dalam suatu data lain untuk "ditumpangi", tetapi orang lain tidak menyadari akan kehadiran adanya data tambahan pada hostnya, sehingga seolah-olah tidak ada perbedaan antara data host sebelum dan sesudah proses *watermarking* [5].

Beberapa aplikasi *watermarking* yang sering digunakan adalah



Gambar 1. Sistem *Watermarking*

a. *Owner identification* (tanda pengenalan kepemilikan)
   Pada aplikasi ini pemilik data dapat menanamkan informasi hak cipta pada data host, sehingga usaha untuk menghilangkan informasi hak cipta akan berdampak menurunnya kualitas data host.

b. *Proof of ownership* (Bukti kepemilikan)
   Selain digunakan sebagai tanda pengenalan pemilikan, *watermarking* juga dapat digunakan sebagai bukti kepemilikan. Pembuktian ini diperlukan bilamana terjadi perselisihan hak kepemilikan atas data digital.

c. *Authentication* (Keaslian)
   Watermarking dapat juga digunakan sebagai teknik untuk membuktikan keaslian suatu data digital. Hal ini disebabkan, *watermark* akan selalu melekat pada data host. Sehingga jika data host mengalami perubahan baik di crooping atau diubah ke dalam format lainnya maka *watermark*nya akan selalu bersama dengan data host.

d. *Fingerprinting*
   Fingerprinting digunakan untuk menelusuri penggandaan ilegal terhadap data host. Pemilik data host dapat menanamkan *watermark* berbeda ke data host yang akan didistribusikan ke pelanggan yang berbeda. Dengan cara ini maka penggandaan ke pihak ketiga akan dapat dideteksi, karena adanya *watermark* yang berbeda untuk pelanggan yang berbeda.

e. *Medical safety*
   Pada aplikasi ini, *watermark* yang berupa data pasien (nama, tanggal) dapat ditanamkan ke data host (medical image) sehingga dapat meminimalisir adanya kesalahan data.

f. *Broadcast Monitoring*
   Pada aplikasi ini *watermark* ditanamkan ke dalam tiap video maupun suara sebelum ditayangkan oleh stasiun televisi atau radio. Untuk itu diperlukan stasiun pengamat otomatis yang akan menerima tayangan tersebut sehingga akan dapat mengekstrak informasi *watermark* yang dibawa dan sekaligus mencatat informasi tayangan yang muncul.

2.2. Kompresi JPEG

Data digital terutama citra memiliki ukuran file yang cukup besar. Hal ini mengakibatkan adanya beberapa permasalahan yang sering terjadi pada pemrosesan citra. Dengan ukuran file yang cukup besar memberi dampak pada ruang penyimpanan dan waktu transfer data. Untuk itu diperlukan upaya kompromi dengan menggunakan kompresi. Sebenarnya kompresi merupakan upaya dilematis. Disatu sisi menguntungkan karena berkurangnya ukuran file tetapi disisi lain merugikan karena menurunnya kualitas citra.

Menurut [6] kompresi dibedakan menjadi dua jenis, yakni *lossless* dan *lossy*. Pada kompresi *Lossless* diperuntukkan ketika terdapat suatu persyaratan bahwa informasi asli tetap utuh. Pesan asli direkontruksi kembali seperti aslinya. Contoh tipe kompresi in adalah citra GIF dan BMP.

Sedangkan kompresi *Lossy* juga menyimpan tempat, tetapi integritas citra asli tidak terjaga. Contoh metode ini terdapat pada citra JPG dan hasil kompresi sangat baik.

Salah satu teknik kompresi standar adalah JPEG yang dibuat oleh *The Joint Photograpic Experts Group*. Kompresi JPEG membagi citra dalam blok yang berukuran 8x8 pixel, kemudian dihitung nilai *Discrete Cosine Transform* (DCT) dari masing-masing blok tersebut. Sebagai input adalah citra asli dalam skala abu-abu A = (0, … , 255) dengan ukuran M x N dan akan menghasilkan citra terkompres dengan ukuran yang sama. Pada kompresi ini terdapat parameter q yang menunjukkan kualitas (quality) kompresi. Nilai q mempunyai rentang 1 sampai 100, dimana 1 menunjukkan tingkat kompresi yang tinggi dengan kualitas yang rendah dan nilai 100 menunjukkan tingkat kompresi yang rendah dengan kualitas yang tinggi. Untuk mengetahui hubungan antara kompresi dengan parameter q dapat digunakan ukuran distorsi [3].

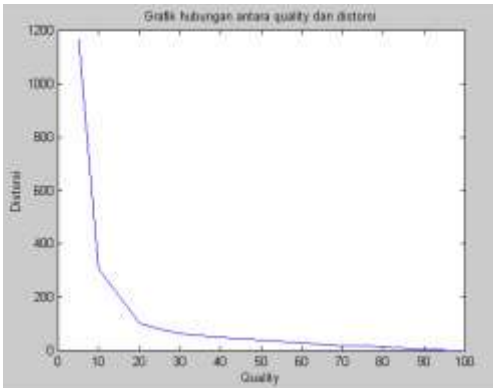
$$Dq = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}(P_{xy} - JPEG_q(P_{xy}))^2, \quad (2.1)$$

dengan

P_{xy} = citra asli pada posisi x,y,

$JPEG_q(P_{xy})$ = citra terkompresi JPEG dengan kualitas q pada posisi x,y.

Selanjutnya hubungan antara kualitas kompresi dengan distorsi pixel citra dapat dilihat pada gambar 2.



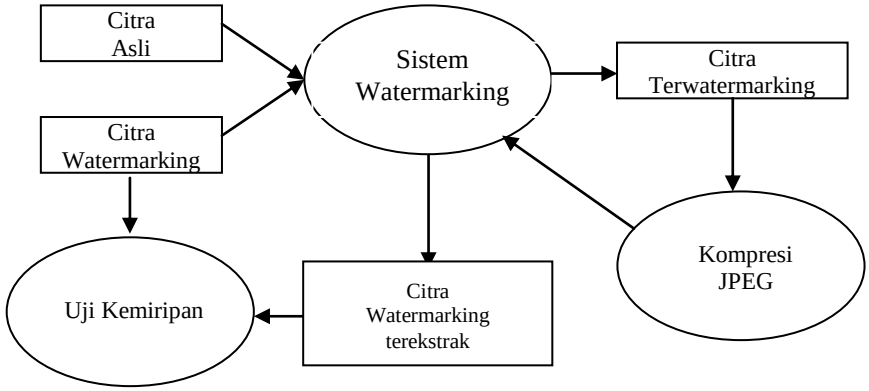
Gambar 2. Grafik hubungan antara quality dan distorsi

3. PEMBAHASAN

3.1. Metode

Pada penelitian ini semua bahan yang digunakan adalah citra digital yang mudah diperoleh diberbagai media. Metode yang digunakan dapat dilihat pada Gambar 3.

Pada tahap awal, citra asli dan citra *watermark* dengan sistem *watermarking* [1] dilakukan proses penanaman sehingga diperoleh citra ter-*watermark*. Selanjutnya citra ter-*watermark* dikenakan serangan kompresi JPEG dengan menggunakan parameter quality tertentu.



Gambar 3. Metode kompresi JPEG dan Uji kemiripan

Kemudian citra ter-*watermark* yang telah terkena serangan kompresi JPEG dengan menggunakan sistem *watermarking* diekstrak untuk memperoleh citra *watermark* terekstrak. Citra *watermark* terekstrak inilah yang akan diuji kemiripannya dengan citra *watermark* asli. Pengujian dilakukan dengan menggunakan rumus *Normalized Cross Correlation* (NC) [4].

$$NC = \frac{\sum_i \sum_j w_{ij} w'_{ij}}{\sum_i \sum_j [w_{ij}]^2} \qquad (2.2)$$

3.2. Hasil

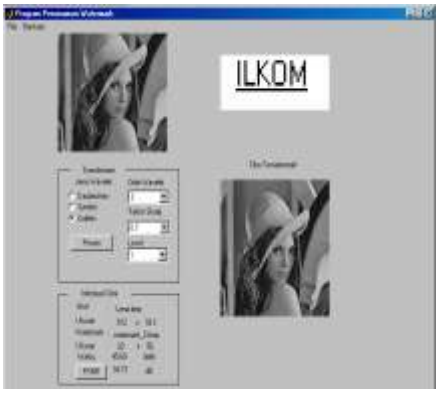
Citra yang disimulasikan adalah citra lena dengan ukuran 512 x 512 dalam skala abu-abu 256 dan citra *watermark*nya merupakan citra biner dengan ukuran 20 x 50. Sedangkan keluarga wavelet yang digunakan untuk transformasi dapat ditentukan sesuai pilihan.

Data-data di bawah ini kemudian disimulasikan dalam sistem *watermarking* dengan menggunakan program aplikasi *Graphical User Interface* (GUI) matlab 6.5 [1] yang diperlihatkan pada Gambar 5.

(a) Citra lena.bmp 512x512

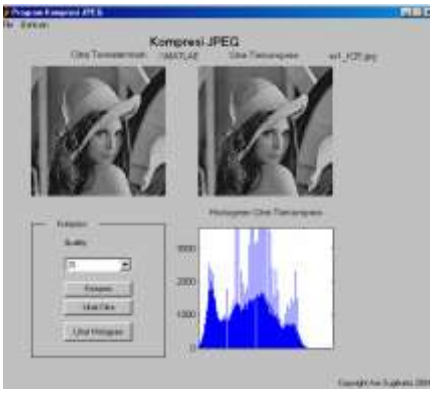
(b) Citra watermark_2.bmp 20x50

Gambar 4. Citra lena dan citra *watermark*_2



(a)

(b)



(c)

(d)

Gambar 5. (a) Penanaman *watermark* ke citra asli, (b) Pengekstrakan *watermark* dari citra ter-*watermark*, (c) Citra ter-*watermark* dari 5.(a) diserang dengan kompresi JPEG (d).Pengekstrakan citra ter-*watermark* 5.(c) .

Host : Lena.bmp [512 x 512]
Watermark : *Watermark*_2.bmp [20 x 50]
Wavelet : Daubechies 4
Level : 1

Tabel 1. Hasil pengujian *watermarking* dengan menggunakan wavelet daubechies 4, *watermark*_2 dan level 1.

Skala	Normalized Cross Corelation (NC)				
	Normal	JPEG25	JPEG50	JPEG75	JPEG100
0.1	0.889396	0.783352	0.781072	0.803877	0.893957
0.5	0.996579	0.833523	0.86203	0.940707	0.996579
1	1	0.872292	0.95553	0.989738	1
1.5	1	0.931585	0.986317	0.986317	1
2	1	0.979475	0.995439	1	1

Host : Lena.bmp [512 x 512]
Watermark : *Watermark*_2.bmp [20 x 50]
Wavelet : Symlets2
Level : 1

Tabel 2. Hasil pengujian *watermarking* dengan menggunakan wavelet Symlet 2, *watermark*_2 dan level 1.

Skala	Normalized Cross Corelation (NC)				
	Normal	JPEG25	JPEG50	JPEG75	JPEG100
0.1	0.871152	0.759407	0.781072	0.77081	0.871152
0.5	0.997719	0.803877	0.859749	0.904215	0.997719
1	1	0.86317	0.938426	0.992018	0.99886
1.5	1	0.91106	0.982896	1	1
2	1	0.963512	0.99886	1	1

Host : Lena.bmp [512 x 512]
Watermark : *Watermark*_2.bmp [20 x 50]
Wavelet : Coiflet3
Level : 1

Tabel 3. Hasil pengujian *watermarking* dengan menggunakan wavelet Coiflet 3, *watermark*_2 dan level 1.

Skala	Normalized Cross Corelation (NC)				
	Normal	JPEG25	JPEG50	JPEG75	JPEG100
0.1	0.887115	0.779932	0.781072	0.795895	0.882554
0.5	0.997719	0.810718	0.871152	0.939567	0.997719
1	1	0.858609	0.95439	0.994299	1
1.5	1	0.924743	0.992018	1	1
2	1	0.970353	0.997719	1	1

Pada Gambar 5.a mula-mula citra asli lena ditanami citra *watermark* ilkom sehingga diperoleh citra ter-*watermark*. Kemudian citra ter-*watermark* tersebut dieks-trak kembali menggunakan sistem yang sama sehingga diperoleh citra *watermark* terekstrak dengan kemiripan NC (normal) = 0.98860. Selanjutnya citra

ter-*watermark* yang diperoleh dari 5.a diserang menggunakan kompresi JPEG dengan parameter quality 25 seperti Gambar 5.c, kemudian citra ter-*watermark* yang telah diserang kompresi JPEG tersebut diekstrak dan diperoleh nilai kemiripan atau NC watermark terekstraknya adalah 0.827822. Secara lengkap dari beberapa percobaan yang dilakukan diperlihatkan pada beberapa tabel berikut.

4. PENUTUP

Dari pembahasan yang telah dilakukan dengan melalui beberapa eksperimen diperoleh kesimpulan bahwa semakin tinggi nilai skala maka kemiripan atau nilai NC juga semakin tinggi. Nilai kemiripan (NC) pada keadaan normal tanpa diserang dengan nilai NC setelah dikenai serangan kompresi JPEG dengan quality 25, 50, 75 dan 100 tidak terlalu jauh berbeda, hal ini menunjukkan bahwa sistem *watermarking* yang digunakan cukup tahan terhadap serangan kompresi JPEG.

5. DAFTAR PUSTAKA

[1] Aris S., Agus H.(2004) ,*Watermarking Citra Digital dengan Transformasi Wavelet Diskrit*, Tesis Magister Ilmu Komputer Universitas Gadjah Mada Yogyakarta.

[2] Aris S., Eko A.S. (2004), *Watermarking Pada Beberapa Keluarga Wavelet*, Jurnal Matematika dan Ilmu Komputer Jurusan Matematika FMIPA UNDIP Semarang, **7**: 18 – 25.

[3] Bandemer Bernd (2003), *Course Project 4 ECE 642, http://www.stud.tuil-menau. de/~beba-ii/docs*.html

[4] Chio-Ting Hsu , Ja-Ling Wu. (1998), *Multiresolution Watermarking for Digital Images*, IEE Trans Circuit & System II: Analog & Digital Signal Processing, **45**: 1097 - 1101.

[5] Cox, I.J, Kilian,J, Miller, M.L, Bloom, J.A. (2000) , *Watermarking Appl-cations and Their Properties,* Proceedings of the Conf. Information Technology.

[6] Munir Rinaldi. (2004), *Pengolahan Citra Digital dengan Pendekatan Algoritmik*, Penerbit Informatika Bandung.